In the Claims

The status of claims in the case is as follows:

1. [Currently amended] A computer implemented method for detecting denial of service attacks, comprising the steps of:

issuing a bit encoded login challenge composed of human viewable images not composed of machine readable text in response to a login request to said computer from a requester of services; and

responsive to an incorrect response to said challenge, said computer placing said requester in a state of limited service.

2. [Previously presented] The computer implemented method of claim 1, further comprising the steps of:

filtering out to said state of limited service iterative connection requests from a network address of a hacker device.

3. [Previously presented] The computer implemented method of claim 1, further comprising the step of:

responsive to speed, latency and average queuing network delay of connection requests, detecting and placing in a state of limited service repetitive login requests from a hacker device.

4. [Previously presented] The computer implemented method of claim 3, further comprising the steps of:

determining from said speed, latency and average queuing network delay a time-out value; and

detecting as a request from a hacker device a request that does not complete within said time-out value.

5. [Previously presented] The computer implemented method of claim 1, further comprising the steps of:

issuing further challenges to subsequent requests for service from said requester and selectively responding to successful responses by continuing service at the same or improved level and to unsuccessful responses by

further reduction or complete denial of service.

6. [Previously presented] The computer implemented method of claim 1, further comprising the steps of:

periodically issuing said challenges throughout connection to a requester successfully responding.

7. [Previously presented] The computer implemented method of claim 1, comprising the step of issuing said bit-mapped challenge as logon image from which a user must select or enter a response.

8. [Previously presented] The computer implemented method of claim 7, further comprising the step of occasionally shifting the input area for a valid response to said challenge.

9. [Previously presented] The computer implemented method of claim 1, further comprising the step of slowing acceptance from and response to systems in a degraded service category.

10. [Previously presented] The computer implemented method

of claim 1, further comprising the step of counterattacking by executing a denial of service response to attacking systems.

11. [Currently amended] A computer implemented method for detecting denial of service attacks, comprising the steps of:

executing a bit-encoded ~~challenge-response~~ challenge and response login procedure and a network probing test frame transmission and analysis procedure to detect a hacker denial of service attack, said bit-encoded challenge comprising human viewable images not composed of machine readable text;

said network probing test frame transmission and analysis procedure including defining a signature of discrete speed, streaming speed, and latency of the connecting device failing said bit-encoded challenge-response login procedure, and adding said signature to a router based filter for filtering out login requests from said hacker responsive to said signature; and

responsive to detecting said denial of service attack,

placing said hacker in a lower level of service state.

12-14. [Canceled]

15. [Currently amended] A computer implemented method for detecting denial of service attacks, comprising the steps of:

selecting sending and receiving probative test packets through a network;

responsive to said packets, determining network evaluation parameters for said network;

responsive to said network evaluation parameters, determining presence of network denial of service attacks, said network evaluation parameters including response time and throughput characteristics of said network, said throughput characteristics including capacity, utilization, and performance; and

executing a ~~challenge-response~~ bit-encoded challenge and response procedure to discourage and repel said attacks, said bit-encoded challenge comprising human

viewable images not composed of machine readable text.

16. [Previously presented] The computer implemented method of claim 15, further comprising the steps of:

determining a latency and speed fingerprint of an offending device;

responsive to said fingerprint, operating a router filtering system to reject packets from said offending device.

17. [Previously presented] The computer implemented method of claim 16, said fingerprint comprising a rhythm of transmissions of discrete, burst, and stream packets.

18-23. [Canceled]

24. [Previously presented] A computer implemented probative test and analysis method for detecting and responding to denial of service attacks on a network resource, comprising the steps of:

creating a template of attack patterns;

determining historical, current, and predicted states of said network for each of a plurality of types of network traffic;

responsive to said attack patterns, determining if a spike in network traffic is a distributed denial of service attack and, if so, determining its source; and

denying full service to sources associated with said service attack.

25. [Previously presented] The computer implemented method of claim 24, further comprising the steps of:

determining unique speed and latency network attachment characteristics of devices attempting to connect to said network resource; and

responsive to detection of an abusive behavior from a said device, responding to subsequent requests for service from said device by denying said full service to said device.

26. [Currently amended] A computer program product for

detecting denial of service attacks, comprising:

a computer readable medium;

first program instructions to issue a bit encoded login challenge comprising human viewable images not composed of machine readable text in response to a login request from a requester of services;

second program instructions, responsive to an incorrect response to said challenge, to place said requester in a state of limited service; and wherein

said first and second program instructions are recorded on said computer readable medium.

27-29. [Canceled]

30. [Currently amended] A computer program product for detecting denial of service attacks, comprising:

a computer readable medium;

first program instructions for executing a network

probing test frame transmission and analysis procedure including requiring response of a user to presentation of human viewable images not composed of machine readable text to detect a hacker denial of service attack;

second program instructions, responsive to detecting a denial of service attack, for placing said hacker in a state of lower level of service; and wherein

said first and second program instructions are recorded on said computer readable medium.

31. [Currently amended] A computer program product for detecting denial of service attacks, comprising:

a computer readable medium

first program instructions to selectively send and receive probative test packets through a network;

second program instructions, responsive to said packets, to determine network evaluation parameters for said network;

third program instructions, responsive to said network evaluation parameters, to determine presence of network denial of service attacks, said network evaluation parameters including response time and throughput characteristics of said network, said throughput characteristics including capacity, utilization, and performance;

fourth program instructions to execute a ~~challenge-response~~ bit-encoded challenge and response procedure to discourage and repel said attacks, said bit-encoded challenge comprising human viewable images not composed of machine readable text; and wherein

said first, second, third, and fourth program instructions are recorded on said computer readable medium.

32. [Previously presented] The computer program product of claim 26, further comprising:

third program instructions for filtering out to said state of limited service iterative connection requests from a network address of a hacker device; and wherein

said third program instructions are recorded on said computer readable medium.

33. [Previously presented] The computer program product of claim 26, further comprising:

third program instructions, responsive to speed, latency and average queuing network delay of connection requests, for detecting and placing in a state of limited service repetitive login requests from a hacker device; and wherein

said third program instructions are recorded on said computer readable medium.

34. [Previously presented] The computer program product of claim 26, further comprising:

third program instructions for determining from said speed, latency and average queuing network delay a time-out value;

fourth program instructions for detecting as a request from a hacker device a request that does not complete

within said time-out value; and wherein

said third and fourth program instructions are recorded on said computer readable medium.

35. [Previously presented] The computer program product of claim 26, further comprising:

third program instructions for issuing further challenges to subsequent requests for service from said requester and selectively responding to successful responses by continuing service at the same or improved level and to unsuccessful responses by further reduction or complete denial of service; and wherein

said third program instructions are recorded on said computer readable medium.

36. [Previously presented] The computer program product of claim 26, further comprising:

third program instructions for periodically issuing said challenges throughout connection to a requester successfully responding; and wherein

said third program instructions are recorded on said computer readable medium.

37. [Previously presented] The computer program product of claim 26, further comprising

third program instructions for issuing said bit-mapped challenge as logon image from which a user must select or enter a response; and wherein

said third program instructions are recorded on said computer readable medium.

38. [Previously presented] The computer program product of claim 37, further comprising

fourth program instructions for occasionally shifting the input area for a valid response to said challenge; and wherein

said fourth program instructions are recorded on said computer readable medium.

39. [Previously presented] The computer program product of

claim 26, further comprising

third program instructions for slowing acceptance from and response to systems in a degraded service category; and wherein

said third program instructions are recorded on said computer readable medium.

40. [Previously presented] The computer program product of claim 26, further comprising

third program instructions for counterattacking by executing a denial of service response to attacking systems; and wherein

said third program instructions are recorded on said computer readable medium.